Securing SMS to increase Information Technology benefits for Remote SSI/MSME’s inside Indian society

Prof. B K Srinivas [#1] & Mr. Ashpaqahmad Nadaf [#2]
[#] Department of Information Science & Engg., RVCE, VTU
Bengaluru, India

Abstract*—Cloud being the latest development in Information Technology can drive the inclusive growth agenda by providing an international platform for SSI/MSME’s. Access to cloud services with the help of mobile phone using SMS (Short message Service) is major concern for SSI/MSME’s located in remote areas.The short message service (SMS) being one of the highly used and well-tried mobile services with global availability within all GSM networks facesecurity as the major issue when entrusting an organization’s critical information to geographically dispersed cloud platforms not under the direct control of that organization.SMS does not have any built-in procedure to authenticate the text and offer security for the text transmitted as data. This paper details the mechanism which can be used to protect the SMS. In addition, paper provides a protocol for secure SMS communication for SSI/MSME’s to harness the cloud computing potential.*

Keywords*— SMS, SSI, MSME, Cloud computing, Remote area, Security, Information Technology, Mobile Communication*

I. Introduction

The usages of electronic devices are increasing day by day due to wireless technology that allows storing personal information easily and effectively. In which Short Messaging Service (SMS) become more popular in the world especially in India due to sudden change of Currency (Notes) in November 2016.Result in Increase the usage of mobile banking, m-commerce. But the main challenge is to secure text and SMS communication. This paper details the mechanism to solve these challenges.

II. Mobile communication

India is the 2nd largest country in telecom market [1]. Evolving mobile technology provides a greater mobile experience. Four generation of mobile communication are1G, 2G, 3G and 4G [2] as shown in Figure 1.

A. 1G Technology

1G is a first established technology for mobile connection that introduces voice services.

B. 2G Technology

2G is digital wireless technology that works on voice signals for transmission of information. 2G technology contains 3 different types: FDMA ,TDMA and CDMA.

FDMA usage provides low quality voice that works with equal spectrum by separating frequency.

Time Division Multiple Access (TDMA) divides band into 3 time periods. It contains GSM technology.

CDMA works with entire band provides separate code for different phones. This allows both receiver and sender to use their codes with full band.

C. 3G Technology

3G network is faster than 2G that is faster download and access to the applications.3G works with the mix of packet switching and circuit switching network.

D. 4G Technology

4G networks works with packet switching which is faster than 3G.but the cost of using 4G is high compared to other generation of technologies.

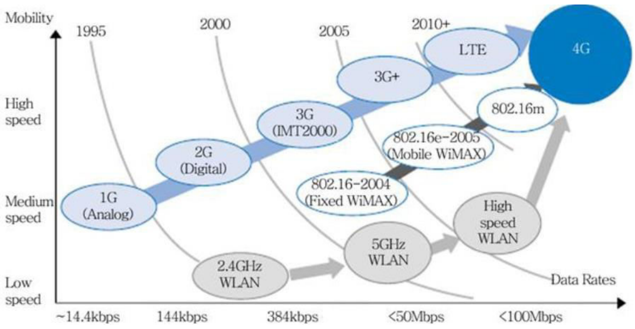


Figure1. Evolution of mobile communication

The Cloud becomes more popular technology for storing personnel information that deliver resources and computing to customers on demand. Cloud uses virtualization concept to reduce the cost being used for resources in information technology.

Global System for Mobile Communication (GSM) includes several features like data connection, voice connection, multi service or basic services. But SMS is a Notable feature of GSM network [2]. It requires the SIM is to initiate communication.

The main purpose of using the SMS is to transmit the information in terms of text messages from one device to another. Hence, it is more important to protect the attacks on SMS in terms of illegal activities to ensure the originality of data. Due to the unencrypted content it is possible to read and write or modify the SMS content by operator's employee. This is obvious because of developer does not take an account to protect the parts of SMS applications. Transmission of SMS is in terms of insecure text mode and through insecure transmitting channels. So security is the main region to protect SMS.

III. SMS Operations

Generally the transmission of SMS goes through several paths and procedures from sender to receiver and both subscriber belongs to one or different mobile operators[3]. Exchanging information where subscribers belongs to same operator show in Figure 2

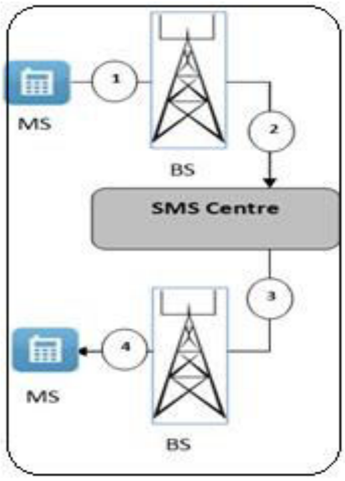


Figure2. SMS transmission by Subscribers belonging to one Mobile operator

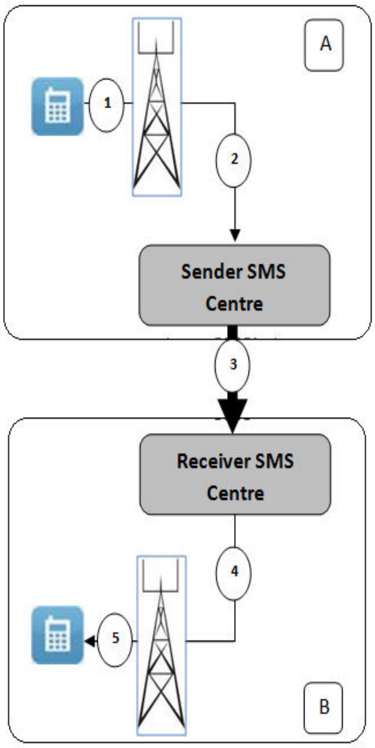


Figure3. SMS transmission by Subscribers belonging to different Mobile operator

When SMS sent from mobile device goes to nearest Base Station (BS) via Interface called On- The-Air(OTA) protocol. Then SMS will be forwarded to the SMSC through BS. When SMS arrived to SMSC it sends the Message to its nearest Base Station over SS7 and finally BS transfer the message to the destination through OTA protocol.

There are several steps for Information exchange between the both subscribers belongs to different Mobile operator. In this case SMS passes through 2 Short Message Service Centre (SMSC). There are two layer in which message will be sent, application layer at the sender and receiver side. Transport layer in between sender and receiver that is in air medium. Hence security is the main concern during SMS transmission. Figure 3 illustrate the exchanging SMS between mobile two different mobile operator subscribers.

Transmitting SMS in which subscribers belonging to different operators work in same manner of with subscriber belong to one operator, but here SMSC at the sender side reformats the message to Short Message Peer to Peer Protocol (SMPP). And afterwards message will be send to SMS gateways using protocol TCP/IP over the private or public internet which links to SMSC at the mobile recipient[3].

IV. Security Concern

Several encryption methods were proposed to ensure the confidentiality and the integrity for content that is to be transmitted and also for safe communication. Authentication can be achieved by installing server at the backend that is connected to SMSC to verify authenticity for finding the ownership of the mobile, and medium to encrypt[4]. Figure 4 illustrate the authentication process for mobile devices.

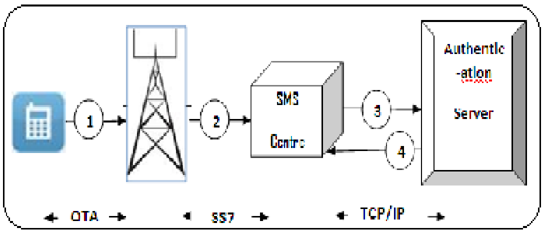


Figure 4. Authentication process for mobile devices.

SMS sent from mobile devices passes to BS via OTA. Then Mobile Switching Centre (MSC) manage SMS between BSs until it reach to SMS centre. SMSC forward SMS for authentication server to verify SMSs Sender through TCP/TP. SMSC enquires the Home Location Registration (HLR) after getting acknowledgement from authentication server to find the target mobile location in mobile network.

A. *At Application layer*

There are several threats or attacks on SMS message during this application layer. Unencrypted Storage in which attacker can read or change the data stored inside SMS inbox of the sender or receiver mobile. Man-in-the-middle attack occurs during the exchanging of public key between both the parties involved in the transaction. Since this is not enough to provide full SMS protection.

B. *At Transport layer*

During transmission of SMS from sender to receiver the attacks can be occurred at transport layer. There are several attacks during the authentication process over OTA interface.SS7 becomes attacker's target because every database queries, call setup, roaming controlled happened in this channel. SMSC will accept any connection without authenticate of machine on the internet.

V. Security Techniques

To avoid the vulnerabilities Communication channel should be protected for both mo bile operators and mobile applications.

A. *Application layer Techniques*

Applications are designed and developed in mobile devices. So it is important to provide end-to-end security. That is protecting the SMS privacy by encrypting and decrypting the message body at the Sender Side and receiver side. Figure 5 illustrate SMS framework which has two fields, SMS payload and header.

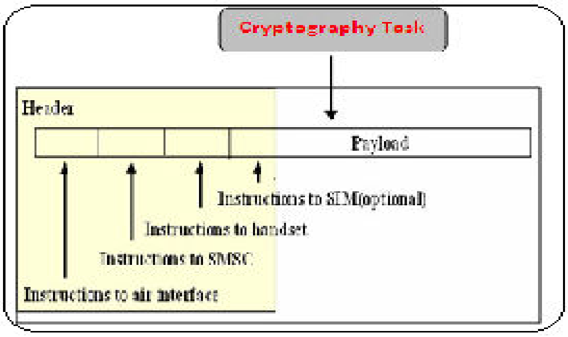
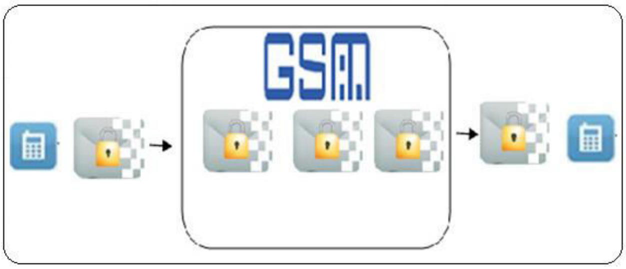


Figure 5 SMS framework

A single SMS consist of 140 bytes and has unique SMS structure and formats for GSM network. The security mechanism needed for the sensitive information contained inside the payload. Cryptographic is a technique that provides tool for protecting sensitive communication over the network. Thus security concepts are applied to SMS header. This requires some special packages which allow accessing the SMS header Figure 6 illustrate the end-to-end security for SMS transmission in communication medium. WMA is a one which is main package and widely used during transmission of SMS.



Figue 6. End-to-end security

There are 3 types of crypto-graphic schemes i) Symmetric cryptography, ii) Asymmetric Cryptography iii) Hash function.

Symmetric cryptography

This is the first technique and high quality solution for SMS protection. To protect the SMS content it shared secret key between two or more communicating parties shown in Figure 7. In this technique key distribution is the main problem because Square of number of keys required than sender and it is not possible to exchange without help of any technique (cryptographic). key exchange should be done in different communicating way where both parties involved in the communication should agree before establishing SMS transmission[5].

GSM
GLOBAL SYSTEM FOR
MOBILE COMMUNICATIONS

Figure 7. Symmetric cryptography

Asymmetric cryptography

Combination of asymmetric and symmetric provides robust functionalities. key agreement problem can be resolve by using two different keys one as a secrete key or private key and other is a public key[6]. Figure 8 illustrate cryptographic process in which communicating patties involved in generating two key pairs. To perform encryption process for plain text the sender need to send his public key or inform to the other communicating parities. Then for decryption process the receiver use his private key to decrypt message. Public key can be distributed openly but Private key should be kept secret. Here, if the Public key used wrongly due to inexperienced operation and protocol doesn't provide any authentication, there may be a chance of MITM attacks. To solve this problem by using third trusted party to determine authenticity of the receiver. Which use Public Key Infrastructure (PKI) as add-on to this authentication scheme in the key exchange process [7].

GSM
GLOBAL SYSTEM FOR
MOBILE COMMUNICATIONS

Figure 8. Asymmetric cryptography

Mobile PKI

It can be used to prevent the keys from MITM attacks and provide secure end-to-end communication among the communicating parties [8]. Figure 11 shows Framework of Mobile PKI for secure transmission. Every mobile user should register public key with trusted party. Trusted party checks weather the key belongs to registrant and accurate information associated with them. Then Certificate will be issued and duly signed by relevant authority. Figure 9 illustrate the process of downloading certificate from CA this is tabulated in Table 1.

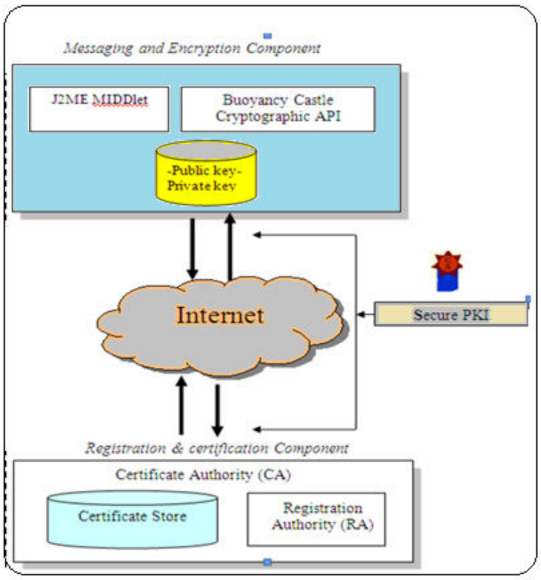

Messaging and Encryption Component
J2ME MIDDlet
Buoyancy Castle Cryptographic API
-Public key-
Private key
Internet
Secure PKI
Registration & certification Component
Certificate Authority (CA)
Certificate Store
Registration Authority (RA)

Figure 9. Download PKI certificate

Table 1. Steps for downloading CA certificate

Figure Location	Description
1	Mobile device send an HTTP request to CA about enquiring the peer certificate
2	CA checks weather the required certificate is available or not and sign it before sending back to the application of mobile user with HTTP response.
3	Application verifies and extracts the public key from received certificate used to secure and store SMS message via asymmetric cryptography to its certificate directory with the help of cryptography algorithms and SMSC techniques.

To Secure SMS transmission every communicating parties should download CA certificate contains digital signature before applying cryptographic mechanism. In the present mobile system, several applications are already been installed on the bases of PKI through the X.509 certificate standards. But it is difficult to install on the every mobile so it need be maintained at the server side. Thus changing or upgrading new certificate will be persisting into every mobile user. Before downloading certificate, install middle server between PKI server and mobile devices as shown in Figure 10.

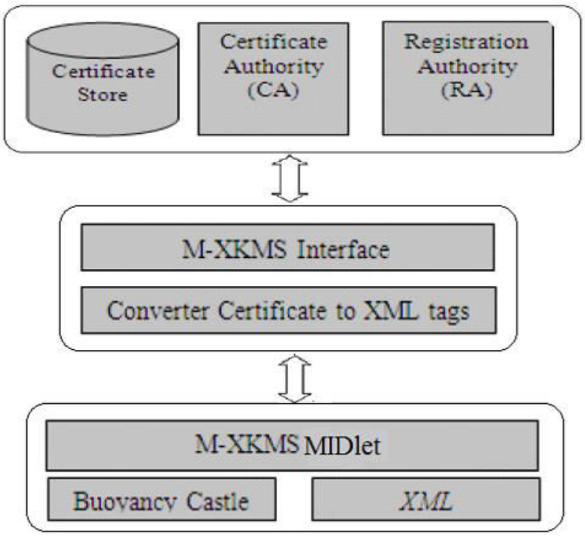

Certificate Store
Certificate Authority (CA)
Registration Authority (RA)
M-XKMS Interface
Converter Certificate to XML tags
M-XKMS MIDlet
Buovancv Castle
XML

Figure 10. Secure SMS transmission

Middleware contains XML key management Specification (XKMS) which is the best solution for the mobile devices (clients). So middleware shield mobile devices from PKI. Thus it can reduce the overhead (complexity) on the mobile devices such as battery issue, high power capability demand and harness to the cloud.

Conclusion

Securing SMS is the main challenge for mobile users and also for Remote SSI/MSME's. This paper reviews, PKI provides high level security to protect SMS during the transmission and secure communication for SSI/MSME's to harness the cloud computing potential.

REFERENCES

[1] V. Devadevan, "Mobile Banking in India-Issues and Challenges", *IJETAE* International Journal of Emerging Technology and Advanced Engineering, vol. 3, pp. 516–520, June. 2013.

[2] Rajasweta Datta, Niharika "Comparative Study between the generation of mobile communication ", *IJRITCC* I International Journal on Recent and Innovation Trends in Computing and Communication, vol. 1, pp. 327–331, Mar 2013.

[3] A. Medani1, A. Gani1, O. Zakaria, A. A. Zaidan and B. B. Zaidan, "Review of mobile short message service security issues and techniques towards the solution", *IJETAE* International Journal of Emerging Technology and Advanced Engineering, vol. 6(6), pp.1147-1165, 18 March, 2011.

[4] N.J Croft and M.S Olivier." Using an approximated One-Time Pad to Secure Short Messaging Service (SMS)", in D Browne (ed), Southern African Telecommunication Networks and Applications Conference, vol. 1, pp.71-76, Sept 2005.

[5] Dankers J, Garefalakis T, Schaffelhofer R, Wright T "Public key infrastructure in mobile systems", *IET Journals & Magazines.* Electronics & Communication Engineering Journal , vol. 14, pp. 180 – 190, Dec 2002.

[6] W. Diffie; M. Hellman " New directions in cryptography", *IEEE* Transactions on Information Theory , vol. 22, pp.644 - 654, Jan 2003.

[7] Jøsang A, Zomai MA, Suriadi S, "Usability and privacy in identity management architectures Proceedings of the Fifth Australasian Symposium on Grid Computing and e-Research , vol. 14, pp. 152, Jun 2007.

[8] Alanazi H, Jalab H, Alam G, Zaidan B, Zaidan A "Full Length Research Paper Securing electronic medical records transmissions over unsecured communications: An overview for better medical governance ", *Journal of Medicinal Plants Research*, vol. 4(19), pp. 2059-2074, Oct 2010.